

IDS 8 sep 5/2002

JAPANESE UNEXAMINED PATENT PUBLICATION (A)

(11) Publication number: 2-287970

(43) Date of publication of application:

28.11.1990

(51) Int.CI.

G11B 20/02

7/00

(21) Application number: (71) Applicant:

1-107533 HITACHI MAXELL LTD.

(22) Date of filing: (72) Inventor:

28.04.1989 TAKAYUKI GOTO

(54) [TITLE OF THE INVENTION] OPTICAL RECORDER

SPECIFICATION

1. TITLE OF THE INVENTION

Optical Recorder

2. CLAIMS

(1) An optical recorder provided with:

a drive means for an optical recording medium;
a modulation/demodulation device for modulation of a
write signal to the optical recording medium and demodulation
of a read signal from the optical recording medium;

a nonvolatile storage means storing an address of a cryptographic code recorded in the optical recording medium and a medium identification code;

a modulation/demodulation control means for reading and comparing said medium identification code from said optical recording medium and nonvolatile storage means, reading the cryptographic code based on the medium identification code when the corresponding medium identification code is stored in said nonvolatile storage means, and controlling the modulation/demodulation method of the modulation/demodulation device using that cryptographic code;

a random pattern generating means for changing an address for recording the cryptographic code each time a recording/reproduction operation ends; and

a system control means for system control of the above devices.

(2) An optical recorder as set forth in claim 1, wherein said nonvolatile storage means is a random access memory (RAM) with a battery backup.

(3) An optical recorder as set forth in claim 1, wherein said nonvolatile storage means is an electrically erasable programmable read only memory (EEPROM).

(4) An optical recorder as set forth in claim 1, wherein said nonvolatile storage means is an IC card.

(5) An optical recorder as set forth in claim 1, wherein said modulation/demodulation control means is comprised by the same microcomputer as said random pattern generating means and system control means.

3. DETAILED DESCRIPTION OF THE INVENTION

(Field of Utilization in Industry)

The present invention relates to an optical recorder for driving an optical recording medium such as an optical disk or an optical card so as to record/reproduce information, more particularly relates to a security means for information recorded on the optical recording medium.

(Prior Art)

An optical recording medium has the feature of a much larger recording capacity than other information recording media, but for this reason itself strict security is demanded in an optical recorder in which such an optical recording medium is loaded for recording/reproduction of confidential information.

In the past, as a security means in optical recording, it has been known to record a cryptographic code in advance at a predetermined position of an optical recording medium and to attach a device to an optical recorder for reading that cryptographic code and judging if that optical recording

medium is suitable for the optical recorder provided with it or if that optical recording medium is the property of the person operating it.

(Problem to be Solved by the Invention)

However, the conventional security means, like for example the ones in practical use in cash cards etc., record a cryptographic code at a predetermined position of the optical recording medium by a predetermined system, so a person having the knowledge and equipment relating to the recording/reproduction of such an optical recording medium could easily read the cryptographic code. Therefore, complete security was not possible.

Accordingly, an object of the present invention is to provide an optical recorder provided with a more advanced security function for information recorded on an optical recording medium.

(Means for Solving the Problem)

To achieve the above object, the present invention provides an optical recorder provided with (1) a drive means for an optical recording medium, (2) a modulation/demodulation device for modulation of a write signal to the optical recording medium and demodulation of a read signal from the optical recording medium; (3) a nonvolatile storage means storing an address of a cryptographic code recorded in the optical recording medium and a medium identification code; (4) a modulation/demodulation control means for reading and comparing said medium identification code from said optical recording medium and nonvolatile storage means, reading the cryptographic code based on the medium identification code when the corresponding medium identification code is stored in said nonvolatile storage means, and controlling the modulation/demodulation method of the modulation/demodulation device using that cryptographic code; (5) a random pattern generating means for changing an address for recording the cryptographic code each time a recording/reproduction operation ends; and (6) a control means for system control of

the above devices.

Further, before starting the recording/reproduction operation with respect to the optical recording medium, the medium identification code is read from the optical recording medium and nonvolatile storage means, judges if the medium identification code stored in the optical recording medium has been registered in the nonvolatile storage means, and prohibits the recording/reproduction operation when it has not been registered. Further, each time a recording/reproduction operation with respect to the optical recording medium ends, the cryptographic code is relocated to an address designated by the random pattern generating means.

(Mode of Operation)

The medium identification code is recorded at a predetermined position in the optical recording medium, so can be easily read. However, even if the medium identification code is known, it is not possible to read the information unless the recording address of the cryptographic code corresponding to that medium identification code is stored in the nonvolatile storage means.

On the other hand, the cryptographic code is changed to a different address of the optical recording medium each time a recording/reproduction operation of the information ends, so even when someone picks up or steals an optical recording medium, he cannot read the cryptographic code and therefore cannot read the information recorded in the optical recording medium.

Therefore, it is possible to achieve an advanced security function.

(Embodiments)

Below, a first embodiment of the present invention will be explained based on FIG. 1 to FIG. 3. The first embodiment of the present invention is characterized by using an optical disk as the optical recording medium and only allowing recording/reproduction of information with respect to a specific optical disk by a specific optical recorder.

FIG. 1 is a block diagram of an optical recorder

according to a first embodiment, wherein 1 is an optical disk, 2 a spindle motor for driving rotation of the optical disk, 3 an optical head for focusing laser or other recording/reproduction light on to a recording surface of the optical disk 1, 4 a modulation/demodulation device of a signal, 5 a microcomputer, 6 a nonvolatile storage means, 7 a display, and 8 a keyboard.

As the optical disk 1, it is possible to use any known optical disk, but as explained in detail later, to prevent a reduction in the recording capacity due to the relocation of the cryptographic code, an optical disk enabling once recorded information to be suitably erased such as a magneto-optic disk or phase change type optical disk is particularly suitable. This optical disk 1 has recorded, as shown in Fig. 2, on its predetermined area where tracking of the optical head 3 can be made, in an optically readable manner at least before the initial recording/reproduction operation a medium identification code 11 for differentiating that optical disk from other similar optical disks and a cryptographic code 12 for designating a modulation/demodulation method of the modulation/demodulation device 4.

Among these, the medium identification code 11 can be formed in relief shapes on the substrate surface at the time of forming the optical disk substrate or can be written on the recording layer by operation of the optical head 3 and modulation/demodulation device 4. On the other hand, the cryptographic code 12 is optically written on the recording layer by operating the optical head 3 and modulation/demodulation device 4.

The modulation/demodulation device 4 is comprised of a reproduction demodulation amplifier 4a for demodulating a read signal from the optical disk 1 and a recording modulation amplifier 4b for modulating a write signal to the optical disk 1 and is designed so that the modulation/demodulation method can be suitably changed by instruction from the microcomputer 5.

The nonvolatile storage means 6 stores the address of

the cryptographic code 12 recorded on the optical disk 1 and the medium identification code 11. It is possible to use a random access memory (RAM) with a battery backup or an electrically erasable programmable read only memory (EEPROM).

The microcomputer 5 is comprised of a modulation/demodulation control means 5a for reading the cryptographic code 12 based on the nonvolatile storage means 6 and controlling the modulation/demodulation method of the modulation/demodulation device 4, a random pattern generating means 5b for changing the address for recording of the cryptographic code 12 each time a recording/reproduction operation ends, and a system control means 5c for system control of the spindle motor 2, optical head 3, and modulation/demodulation device 4.

Next, the operation of the optical recorder according to this embodiment will be explained with reference to FIG. 3.

First, when the optical disk 1 to be used is loaded onto the spindle motor 2 and the keyboard 8 is operated to issue an instruction for driving the optical disk 1, the spindle motor 2 is started up and the optical disk 1 is driven based on a program stored in the system control means 5c (step S-1).

Next, the optical head 3 is driven to a write position of the medium identification code 11 based on a program stored in the system control means 5c and the medium identification code 11 is read (step S-2).

When the medium identification code 11 has already been written in the optical disk 1, the medium identification code 11 read from the optical disk 1 and the medium identification code stored in the nonvolatile storage means (hereinafter referred to as the "nonvolatile memory") 6 are compared and it is judged if the medium identification code 11 of the loaded optical disk 1 has been registered in the nonvolatile memory 6 (step S-4).

When registered, the address information of the cryptographic code corresponding to the medium identification code 11 is read from the nonvolatile memory 6 (step S-5).

Next, the optical head 3 is driven in accordance with that address information and the cryptographic code recorded on the optical disk 1 is read (step S-6).

The modulation/demodulation control means 5a recognizes the modulation/demodulation method suitable for the optical disk 1 from that cryptographic code 12 and controls the modulation/demodulation method of the modulation/demodulation device 4 (step S-7).

Next, the information is recorded/reproduced based on the modulation/demodulation method (step S-8).

When the keyboard 8 is operated to instruct the end of the predetermined recording/reproduction operation, the random pattern generating means 5b designates a new address of the optical disk for writing the cryptographic code 12, and the optical head 3 accesses that address (step S-10).

When that address is empty, the recording modulation amplifier 4b is driven to write the cryptographic code 12 (step S-12) and that address is registered in the nonvolatile memory 6 (step S-13).

Finally, the previous written cryptographic code is erased, the optical disk 1 is ejected, and the system is shut down.

When a cryptographic code 12 has already been written at the new cryptographic code write address, the random pattern generating means 5b designates a new address for writing the cryptographic code 12 again and the cryptographic code 12 is written there (step S-14). After this, that address is registered in the nonvolatile memory 6 and the system is shut down.

When other data is written at the new cryptographic code write address, that data is evacuated to for example an alternate sector (step S-15). A pseudo pattern is generated at that portion where the related data was written and the cryptographic code is contained in that pattern to record the cryptographic code 12 at step S-12. After this, the address is registered in the nonvolatile memory 6 and the system is shut down.

When optical disk is of a type where the medium identification code 11 is later written, the optical disk 1 is a new one, and the medium identification code 11 is not yet written in a predetermined area of it, the optical head 3 and the recording modulation amplifier 4a are driven based on a program stored in the system control means 5c, the medium identification code 11 is written in that predetermined area (step S-16), and that medium identification code 11 is registered in the nonvolatile memory 6 (step S-17). Further, the random pattern generating means 5b designates an address on the optical disk for writing the cryptographic code 12 (step S-19), the cryptographic code 12 automatically determined by the system at step S-18 is written at that address, and the address is registered in the nonvolatile memory 6 (step S-20).

Next, the modulation/demodulation method of the modulation/demodulation device 4 is controlled by the cryptographic code 12 and the information is recorded/reproduced (step S-7).

When the medium identification code 11 read from the optical disk 1 is not registered in the nonvolatile memory 6, it is not possible to read the cryptographic code of the optical disk from the nonvolatile memory 6 and therefore the recording/reproduction operation of information with respect to the optical disk is automatically prohibited (step S-21).

The optical recorder of this embodiment stores the medium identification code 11 and recording address of the cryptographic code 12 in the nonvolatile memory 6 and checks if the loaded optical disk has been registered in the nonvolatile memory 6, so an optical disk which has not been registered in the nonvolatile memory 6 cannot be used for recording/reproduction of information.

Further, since the recording address of the cryptographic code is changed each time a predetermined recording/reproduction operation ends, it is difficult to decipher the cryptographic code from the optical recording medium and difficult to use an apparatus other than the

predetermined optical recorder to record/reproduce information.

Therefore, an advanced security function can be exhibited.

Note that in the above embodiment, the explanation was made of the case of use of a RAM with a battery backup or EEPROM provided in the optical recorder as the nonvolatile storage means 6, but it is also possible to use second information recording medium, such as an IC card or magnetic card, able to be separately managed from the optical disk.

That is, as shown in FIG. 4, instead of the nonvolatile memory 6, a reader/writer 21 may be connected to the microcomputer 5 and a second information recording medium 22 is loaded into this reader/writer 21 to store the address of the cryptographic code and the medium identification code.

By doing this, it is not possible to record/reproduce information without both of the optical disk and the second information recording medium, so the optical disk is used only by the individual user managing the above information recording media.

Further, in the above embodiment, the explanation was made of the example of an optical disk device, but the present invention is not limited to this in its gist. It is also possible to apply the invention to another optical recorder such as an optical card device recording/reproducing information using an optical card.

Further, in the above embodiment, the explanation was made of an example where the modulation/demodulation control means 5a, the random pattern generating means 5b, and the system control means 5c were comprised by the same microcomputer, but the present invention is not limited to this in its gist. It is also possible to comprise these means by separate microcomputers.

(Effects of the Invention)

As explained above, according to the present invention, only an optical recorder stored in a nonvolatile storage means in advance or only user can use the optical recording

medium. Further, it is difficult to decipher the cryptographic code from the optical recording medium. Therefore, it is possible to exhibit an advanced security function.

4. BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of an optical recorder according to a first embodiment of the present invention; FIG. 2 is a plan view of an optical disk; FIG. 3 is a flow chart explaining the operation of the optical recorder according to the first embodiment; and FIG. 4 is a block diagram of an optical recorder according to a second embodiment of the present invention.

1... ... optical disk, 2... ... spindle motor, 3... ... optical head, 4... ... modulation/demodulation device, 5... ... microcomputer, 6... ... nonvolatile storage means, 7... ... display, 8... ... keyboard, 11... ... medium identification code, 12... ... cryptographic code, 21... ... reader/writer, 22... ... second information recording medium.

FIG. 1

- 1... OPTICAL DISK
- 2... SPINDLE MOTOR
- 3... OPTICAL HEAD
- 4... MODULATION/DEMODULATION DEVICE
- 5... MICROCOMPUTER
- 6... NONVOLATILE MEMORY
- 7... DISPLAY
- 8... KEYBOARD

FIG. 3 (PART 1)

START

- S-1. DRIVE OPTICAL DISK
- S-2. READ MEDIUM IDENTIFICATION CODE
- S-3. CODE ALREADY REGISTERED?
- S-4. ALREADY REGISTERED IN NONVOLATILE MEMORY?
- S-5. READ ADDRESS INFORMATION
- S-6. READ CRYPTOGRAPHIC CODE
- S-7. CONTROL MODULATION/DEMODULATION METHOD
- S-8. RECORD/REPRODUCE INFORMATION
- S-21. STOP RECORDING/REPRODUCTION

FIG. 3 (PART 2)

- S-9. SELECT END MODE
 - S-10. DESIGNATE ADDRESS
 - S-11. NOT YET RECORDED?
 - S-12. WRITE CRYPTOGRAPHIC CODE
 - S-13. REGISTER ADDRESS
 - S-14. CRYPTOGRAPHIC CODE?
 - S-15. EVACUATE TO ALTERNATE SECTOR
- END

FIG. 3 (PART 3)

- S-16. WRITE MEDIUM IDENTIFICATION CODE
- S-17. REGISTER MEDIUM IDENTIFICATION CODE
- S-18. SET CRYPTOGRAPHIC CODE
- S-19. DESIGNATE ADDRESS

S-20. REGISTER ADDRESS

⑫ 公開特許公報 (A) 平2-287970

⑬ Int. Cl.³
G 11 B 20/02
7/00

識別記号 Z 7736-5D
Q 7520-5D

⑭ 公開 平成2年(1990)11月28日

審査請求 未請求 請求項の数 5 (全6頁)

⑮ 発明の名称 光記録装置

⑯ 特 願 平1-107533
⑰ 出 願 平1(1989)4月28日

⑱ 発明者 後藤 隆行 大阪府茨木市丑寅1丁目1番88号 日立マクセル株式会社
内

⑲ 出願人 日立マクセル株式会社 大阪府茨木市丑寅1丁目1番88号

⑳ 代理人 弁理士 武 頸次郎

明細書

1. 発明の名称

光記録装置

2. 特許請求の範囲

(1) 光記録媒体の駆動手段と、

光記録媒体への書き込み信号の変調と光記録媒体からの読み出し信号の復調とを行う変調／復調装置と、

光記録媒体に記録された暗号コードのアドレスおよび媒体識別コードを記憶した不揮発性の記憶手段と、

前記光記録媒体および不揮発性の記憶手段から前記媒体識別コードを読み出して比較し、該当する媒体識別コードが前記不揮発性の記憶手段に記憶されている場合には当該媒体識別コードから暗号コードを読み出し、当該暗号コードをもつて前記変調／復調装置の変復調方式を制御する変復調制御手段と、

記録／再生動作が終了することに、暗号コードを記録すべきアドレスを変更するランダムバタ

ン発生手段と、

前記各装置のシステムコントロールを行うシステム制御手段とを、

具備したことを特徴とする光記録装置。

(2) 請求項1記載において、前記不揮発性の記憶手段がバッテリバックアップ付きのランダムアクセスメモリ(RAM)であることを特徴とする光記録装置、

(3) 請求項1記載において、前記不揮発性の記憶手段が電気消去型プログラマブル読み出し専用メモリ(EEPROM)であることを特徴とする光記録装置。

(4) 請求項1記載において、前記不揮発性の記憶手段がICカードであることを特徴とする光記録装置。

(5) 請求項1記載において、前記変復調制御手段が前記ランダムパターン発生手段およびシステム制御手段と同一のマイクロコンピュータで構成されていることを特徴とする光記録装置。

3. 発明の詳細な説明

【産業上の利用分野】

本発明は光ディスクや光カードなどの光記録媒体を駆動して情報の記録／再生を行う光記録装置に係り、特に、光記録媒体に記録された情報の機密保持手段に関するもの。

【従来の技術】

光記録媒体は他の情報記録媒体に比べて格段に記録容量が大きいという特徴を有するが、それだけにこの光記録媒体を装着して機密性の情報の記録／再生を行う光記録装置には、嚴重な機密保持機能が要求される。

従来、光記録の機密保持手段としては、光記録媒体の一定位置に予じめ暗号コードを記録しており、光記録装置にこの暗号コードを読み出して当該光記録媒体がこれを装着した光記録装置に適合するか否か、あるいは当該光記録媒体がこれを操作する者の所有物であるか否かを判断する装置を付設したものが知られている。

【発明が解決しようとする課題】

然るに、従来の機密保持手段は、例えばキヤウ

シユカードなどで実用化されているものと同様に、光記録媒体上の一定位置に一定の方式で暗号コードを記録しておくというものであるため、光記録媒体の記録／再生に関する知識と装置をもつている者には容易に暗号コードを読み出すことが可能で、完全な機密保持を図ることができない。

従つて、本発明の目的は、光記録媒体に記録された情報のより高度な機密保持機能を備えた光記録装置を提供するにある。

【課題を解決するための手段】

本発明は、前記の目的を達成するため、光記録装置に、①光記録媒体の駆動手段と、②光記録媒体への書き込み信号の変調と光記録媒体からの読み出し信号の復調とを行う変調／復調装置と、③光記録媒体に記録された暗号コードのアドレスおよび媒体識別コードを記憶した不揮発性の記憶手段と、④前記光記録媒体および不揮発性の記憶手段から前記媒体識別コードを読み出して比較し、該当する媒体識別コードが前記不揮発性の記憶手段に記憶されている場合には当該媒体識別コード

から暗号コードを読み出し、当該暗号コードをもつて前記変調／復調装置の変復調方式を制御する変復調制御手段と、⑤記録／再生動作が終了するごとに暗号コードを記録すべきアドレスを変更するランダムパターン発生手段と、⑥前記各装置のシステムコントロールを行う制御手段とを具備した。

そして、光記録媒体に対する記録／再生操作を開始するに先立ち、光記録媒体および不揮発性の記憶手段から媒体識別コードを読み出して光記録媒体に記憶された媒体識別コードが不揮発性の記憶手段に登録されたものであるか否かを判断し、登録されていない場合には記録／再生動作を禁止する。また、光記録媒体に対する記録／再生操作が終了するごとに、ランダムパターン発生手段によつて指定されたアドレスに暗号コードを移し換える。

【作用】

媒体識別コードは光記録媒体の一定位置に記録されているので、容易に読み出すことができる。

しかし媒体識別コードが判つたとしても不揮発性の記憶手段に当該媒体識別コードに対応する暗号コードの記録アドレスが記憶されていなければ情報を読み出すことができない。

一方、暗号コードは、情報の記録／再生が終了するごとに光記録媒体の異なるアドレスに変更されるので、光記録媒体を拾つたり置んだ場合にも暗号コードを読み出すことができず、従つて光記録媒体に記録された情報を読み出すことができない。

よつて、高度な機密保持機能を発揮することができる。

【実施例】

以下、本発明の第1実施例を第1図ないし第3図に基づいて説明する。本発明の第1実施例は、光記録媒体として光ディスクを用い、特定の光ディスクについては特定の光記録装置でしか情報の記録／再生ができないようにしたことを特徴とする。

第1図は第1実施例に係る光記録装置のプロフ

ク図であつて、1は光ディスク、2は光ディスクを回転駆動するスピンドルモータ、3はレーザなどの記録／再生用光を光ディスク1の記録面に合焦する光学ヘッド、4は信号の変調／復調装置、5はマイクロコンピュータ、6は不揮発性の記憶手段、7はディスプレイ、8はキーボードを示している。

前記光ディスク1としては、公知に属する任意の光ディスクを用いることができるが、後に詳述するように暗号コードの移し換えに伴う記録容量の減少を防止するため、例えば光磁気ディスクや相変化形光ディスクなど、一旦記録された情報を適宜消去可能な光ディスクが特に好適である。この光ディスク1には、第2図に示すように、少なくとも最初の記録／再生操作に先立つて、光学ヘッド3をトラシキング可能な一定の領域に、当該光ディスクを他の同種の光ディスクから区別するための媒体識別コード11と、変調／復調装置4の変調／復調方式を指定する暗号コード12とが光学的に読み出し可能な態様で記録される。

段6から暗号コード12を読み出して変調／復調装置4の変復調方式を制御する変復調制御手段5aと、記録／再生動作が終了するごとに暗号コード12を記録すべきアドレスを変更するランダムパターン発生手段5bと、前記スピンドルモータ2、光学ヘッド3、変調／復調装置4のシステムコントロールを行うシステム制御手段5cとから構成されている。

以下、前記実施例に係る光記録装置の動作を第3図により説明する。

まず、使用しようとする光ディスク1をスピンドルモータ2に装着し、キーボード8を操作して光ディスク1を駆動する指令を出すと、システム制御手段5cに記憶されたプログラムに基づいてスピンドルモータ2が起動され、光ディスク1が駆動される(ステップS-1)。

次に、システム制御手段5cに記憶されたプログラムに基づいて光学ヘッド3が媒体識別コード11の書き込み位置まで駆動され、媒体識別コード11の読み出しが行われる(ステップS-2)。

このうち、媒体識別コード11は、光ディスク基板の成形時に基板表面の凹凸の形で形成することができるし、光学ヘッド3および変調／復調装置4を操作して記録層に書き込むことができる。一方、暗号コード12は、光学ヘッド3および変調／復調装置4を操作して光学的に記録層に書き込まれる。

変調／復調装置4は、前記光ディスク1からの読み出し信号を復調する再生復調アンプ4aと、前記光ディスク1への書き込み信号を変調する記録変調アンプ4bとから成り、マイクロコンピュータ5からの指令によって適宜変調／復調方式を変更できるようになっている。

不揮発性の記憶手段6は、光ディスク1に記録された暗号コード12のアドレスと媒体識別コード11を記憶するものであつて、バッテリバックアップ付きのランダムアクセスメモリ(RAM)や電気消去型プログラマブル読み出し専用メモリ(EEPROM)を用いることができる。

マイクロコンピュータ5は、不揮発性の記憶手

光ディスク1に媒体識別コード11が既に書き込まれている場合には、光ディスク1から読み出された媒体識別コード11と不揮発性の記憶手段(以下、不揮発メモリという。)6に記憶された媒体識別コードとを比較し、装着された光ディスク1の媒体識別コード11が不揮発メモリ6に登録されているか否かの判断が行われる(ステップS-4)。

登録されている場合には、不揮発メモリ6から当該媒体識別コード11に対応する暗号コードのアドレス情報を読み出す(ステップS-5)。

次いで、このアドレス情報に従つて光学ヘッド3を駆動し、光ディスク1に記録された暗号コードを読み出す(ステップS-6)。

変復調制御手段5aは、この暗号コード12から当該光ディスク1に適合する変復調方式を認識し、変調／復調装置4の変復調方式を制御する(ステップS-7)。

以下、この変復調方式をもつて情報の記録／再生を行う(ステップS-8)。

キーボード8を操作し、所定の記録／再生動作が終了したことを指示すると、ランダムパターン発生手段5bによって暗号コード12を書き込むべき新たな光ディスクのアドレスが指定され、そのアドレスに光学ヘッド3がアクセスされる（ステップS-10）。

そのアドレスが空いて場合には、記録変調アンプ4bを駆動して暗号コード12を書き込み（ステップS-12）、そのアドレスを不揮発メモリ6に登録する（ステップS-13）。

最後に、先に書き込まれていた暗号コードを消去し、光ディスク1を排出してシステムを終了する。

新たな暗号コード書き込みアドレスに既に暗号コード12が書き込まれている場合には、再度ランダムパターン発生手段5bによって暗号コード12を書き込むべき新たなアドレスを指定し、暗号コード12を書き込む（ステップS-14）。以下、そのアドレスを不揮発メモリ6に登録し、システムを終了する。

アドレスにステップS-18でシステムが自動的に決定した暗号コード12を書き込むと共に、そのアドレスを不揮発メモリ6に登録する（ステップS-20）。

以下、この暗号コード12によって変調／復調装置4の変復調方式を制御し、情報の記録／再生を行う（ステップS-7）。

光ディスク1から読み出された媒体識別コード11が不揮発メモリ6に登録されていない場合には、不揮発メモリ6から当該光ディスクの暗号コードを読み出すことができず、従つて当該光ディスクに対する情報の記録／再生が自動的に禁止される（ステップS-21）。

前記実施例の光記録装置は、不揮発メモリ6に媒体識別コード11と暗号コード12の記録アドレスとを記憶しておき、装着された光ディスクが不揮発メモリ6に登録されたものであるか否かをチェックするようにしたので、不揮発メモリ6に登録されていない光ディスクは情報の記録／再生を行うことができない。

新たな暗号コード書き込みアドレスに他のデータが書き込まれている場合には、そのデータを例えれば交替セクタ等に退避させ（ステップS-15）、開いた部分に擬似パターンを発生してそのパターン内に暗号コードを埋め込み、ステップS-12で暗号コード12を記録する。以下、そのアドレスを不揮発メモリ6に登録し、システムを終了する。

媒体識別コード11を後から書き込むタイプの光ディスクであつて、当該光ディスク1が新品であり、所定のエリアに未だ媒体識別コード11が書き込まれていない場合には、システム制御手段5cに記憶されたプログラムに基づいて光学ヘッド3および記録変調アンプ4aを駆動し、当該所定のエリアに媒体識別コード11を書き込む（ステップS-16）と共に、その媒体識別コード11を不揮発メモリ6に登録する（ステップS-17）。また、ランダムパターン発生手段5bによって暗号コード12を書き込むべき光ディスク上のアドレスを指定し（ステップS-19）、その

また、所望の記録／再生操作が終了するごとに暗号コードの記録アドレスに変更するようにしたので、光記録媒体から暗号コードを解読することが難しく、所定の光記録装置以外の装置を用いて情報の記録／再生を行うことが難しい。

よつて、高度な機密保持機能を発揮することができる。

なお、前記実施例においては、不揮発性の記憶手段6として光記録装置内に設けられたパッテリバックアップ付きのRAMやEEPROMを用いた場合について説明したが、これに代えて例えはI Cカードや磁気カードなど、光ディスクと別個に管理可能な第2の情報記録媒体を用いることもできる。

すなわち、第4図に示すように、不揮発メモリ6に代えてリーダーライター21をマイクロコンピュータ5に接続し、このリーダーライター21に第2の情報記録媒体22を装着することによつて暗号コードのアドレスと媒体識別コードとを記憶させる。

このようにすると、光ディスクと第2の情報記録媒体の双方がない限り情報の記録／再生を行うことができないので、これらの情報記録媒体を管理するユーザ個人にしかその光ディスクを使用できないようにすることができる。

また、前記実施例においては光ディスク装置を例にとって説明したが、本発明の要旨はこれに限定されるものではなく、光カードを用いて情報の記録／再生を行う光カード装置など他の光記録装置にも応用することができる。

さらに、前記実施例においては変復調制御手段5aとランダムパターン発生手段5bとシステム制御手段5cとを同一のマイクロコンピュータにて構成した場合を例にとって説明したが、本発明の要旨はこれに限定されるものではなく、前記各手段を別個のマイクロコンピュータにて構成することもできる。

〔発明の効果〕

以上説明したように、本発明によれば、予じめ不揮発性の記憶手段に記憶された光記録装置もし

くはユーザしか光記録媒体を使用することができず、また、光記録媒体から暗号コードを解読することが困難であることから、高度な権限保持機能を発揮することができる。

4. 図面の簡単な説明

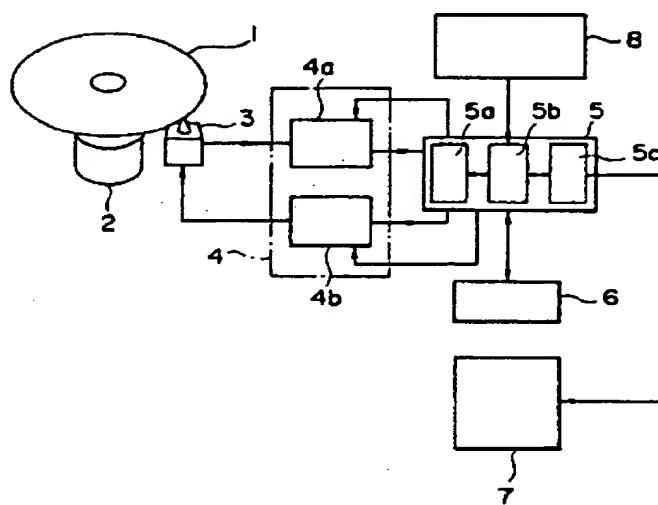
第1図は本発明の第1実施例に係る光記録装置のプロック図、第2図は光ディスクの平面図、第3図は第1実施例に係る光記録装置の動作を説明する流れ図、第4図は本発明の第2実施例に係る光記録装置のプロック図である。

1 ……光ディスク、2 ……スピンドルモータ、
3 ……光学ヘッド、4 ……変調／復調装置、
5 ……マイクロコンピュータ、6 ……不揮発性の
記憶手段、7 ……ディスプレイ、8 ……キーボード、
11 ……媒体識別コード、12 ……暗号コード、
21 ……リーダーライター、22 ……第2の
情報記録媒体。

代理人弁理士 武 誠次郎

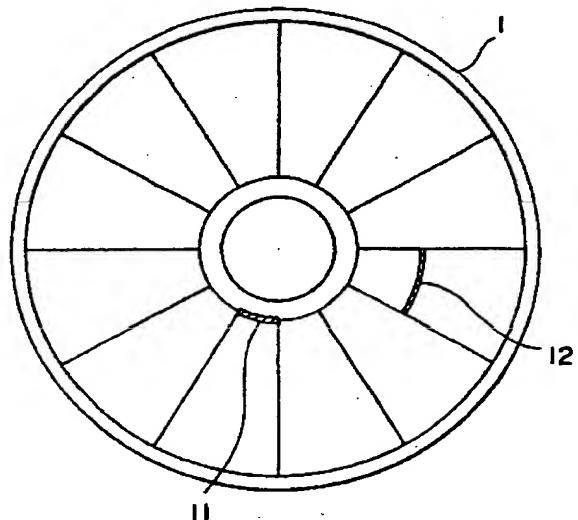


第1図



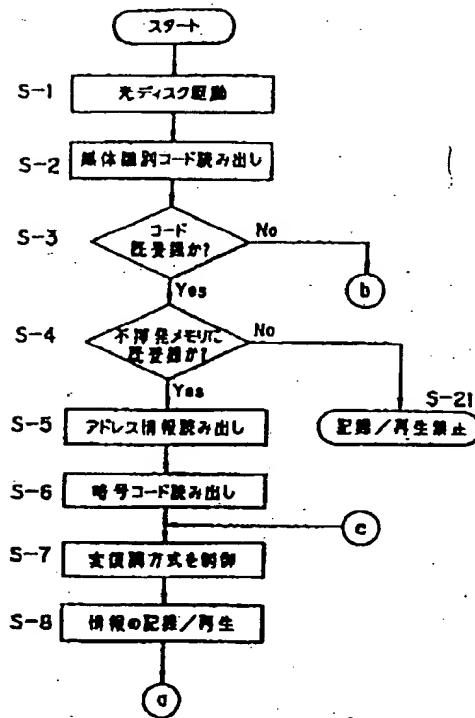
- | | |
|-------------|---------------|
| 1. 光ディスク | 5. マイクロコンピュータ |
| 2. スピンドルモータ | 6. 不揮発メモリ |
| 3. 光学ヘッド | 7. ディスプレイ |
| 4. 変調/復調装置 | 8. キーボード |

第2図

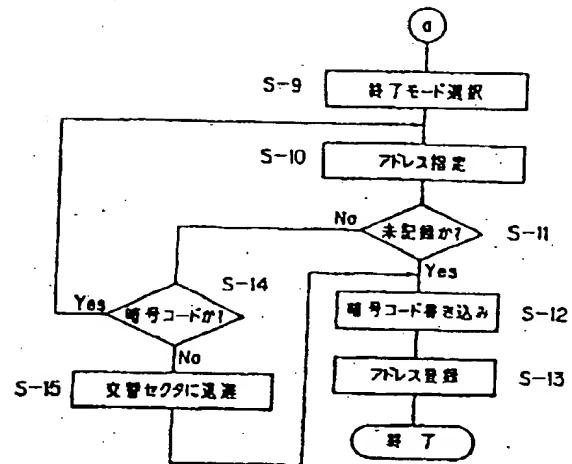


特開平2-287970(6)

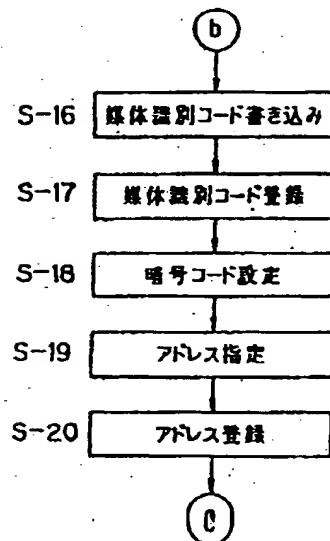
第3図(その1)



第3図(その2)



第3図(その3)



第4図

